Contest «Crowdsource Voting Audit Solutions for Latin American Elections»

Concept of «Digital Voting Audit (Guatemala)» System

Authors: Igor Kholkin, Boris Pimonenko, Roman Nguyen

Table of Contents

1. The Goal and Objectives of the Concept Development

1.1. The Goal of the Concept Development

The goal of the concept development is to form the necessary and sufficient information for deciding on the development or improvement of an IT solution (further - the System), which ensures the improvement of the existing situation in the subject area of the civil (public) audit of election results in Guatemala (hereinafter referred to as the subject area).

Such a concept should describe how to eliminate any possible inconsistencies in the counting of votes and to exclude the possibility of manipulation of the counting votes and auditing process. In other words, the concept should describe how to make the counting and verification of voting results error-free and expedite the provision of information on voting results to civil society in the Republic of Guatemala.

1.2. Objectives of the Concept Development

To achieve established goal, it must:

- describe the initial situation in the subject area;
- identify and analyze the requirements that have arisen because of the presence of problems in the subject area, and address these requirements to the future System;
- form a list of the main capabilities of the future System;
- formulate in one or several versions the vision of the future System that implements the necessary and sufficient list of possibilities;
- evaluate the feasibility of the proposed concept in terms of the functionality of the System and other parameters important for improving the subject area.
- develop a final concept document submitted to the Free TON contest «Crowdsource Voting Audit Solutions for Latin American Elections».

2. Results of The Analysis of the Initial Situation in the Subject Area

The initial situation in the subject area (Case study in Guatemala for the post-election audit of paper ballot election results documents in real-time) is described on the Government Blockchain Association (GBA) portal: https://www.gbaglobal.org/fiscal_digital_2020/ Below is the analysis of this situation:

1. The existing method of auditing voting results in the Republic of Guatemala has problems and disadvantages that lead to a loss of voter confidence and problems with public administration.
2. These disadvantages are associated with an outdated electoral system in which only one paper official document is trusted (Documento Electorale No.4, Acta Final Cierre y Escrutinios (Acta No. 4).
3. Scanned images of Acta №4 are submitted to observers / witnesses (called Fiscal) at Voting Centers on a flash drive, which means the possibility of potential fraud.
4. Falsifications are also manifested when duplicating paper copies of this Acta №. 4. An attempt to avoid counterfeiting by providing a «paper trail» with enough handwritten, site-certified copies for wide distribution and verification has resulted in over 1.5 million paper copies of Acta №4 with various errors in the country. The result was chaos on social media, where attackers could easily alter the digitized images of these documents, fueling distrust of the election.
5. In this regard, the Supreme Court of Elections, Tribunal Supremo Electoral (TSE) formally overturned any legality of handwritten copies of Acta № 4, destroying the «paper trail» that TSE itself does not directly control. The inconsistency between the many paper copies of Acta №4 and their fake social media copies damaged TSE's reputation. At the same time, the problem of the impossibility of verifying the huge number of signed Acta № 4 by the public remains.
6. The next problem is placed in the system of publication of the preliminary election results in the Republic of Guatemala (Sistema de Transmisión de Resultados Preliminares - SITREP). In this system, a paper copy of Acta №4 is given to volunteers, one of many temporary staff at each voting center (they are hired by TSE's IT department). He, having a laptop, a scanner, and a modem, creates a digitized image of Acta №4 in JPG format, and sends it to the TSE database. These files go through several private databases created by private contractors of the TSE IT department. These files are then reviewed, checked, and revised by hundreds of more temporary workers in the TSE data center, and as a result, are published on the TSE website in the preliminary results section. The navigation on the site is confusing, it often breaks down, the site is subject to frequent changes - all this only confuses citizens.
7. To improve the situation, the open-source software Fiscal_Digital was developed. In it, the digitized images of Acta № 4, available to the public through the TSE preliminary results database, were hashed and placed on the Fiscal_Digital blockchain, allowing anyone with a computer, cellphone, and Internet access to participate in a crowdsourced OCR to create an independent vote count. However, such a system relies only on volunteers does not guarantee a complete check of all Acta №4 - it only partially solves the problem.

8. As a result, few people in the Republic of Guatemala now trust the electoral bodies, most of the citizens puts questioned the legitimacy of the elections, leading to increased governance problems for the new government elected in 2019.

Significant improvements are needed in the current situation in the field of verification (audit) and public presentation of the results of the elections.

3. Requirements for Improving the Situation

3.1. Initial Conditions

The primary source of voting data is Documento Electorale №4, Acta Final Cierre y Escrutinios (Acta №4), an official legally significant document - the final summary act on the results of voting at a specific voting table of a particular voting center. This is the only document on the results of voting that is legally recognized in the Republic of Guatemala.

3.2. Requirements

Here are the requirements for improving the existing situation in the field of verification (audit) and public presentation of the results of the elections:

1. The solution should ensure the elimination of the problems specified in section 2, and contribute to the restoration of voters' confidence in the elections, provide an opportunity to move from the current state of distrust to a state of reasonable trust in the election results, eliminating the possibility of their falsification.
2. The decision should contain technologies, methods, models, measures to ensure the ability to minimize errors in vote counting, and subsequent audit.
3. The decision must be implemented within the existing electoral system without the need for any legislative interference from the government. Election legislation and actual voting processes cannot be changed.
4. The solution must be decentralized, i.e. not dependent on any government agency or political party.
5. The solution should provide for the means of counteracting possible attacks from election fraudsters, and the ways of their opposition to the proposed IT solution.

A description of a System that meets the above requirements is given in the next section.

4. General Description of the System

4.1. Purpose of the System

The name of the System is «Digital Voting Audit Guatemala».
The purpose of the System is a public online check / audit and analysis of voting results based on official information from the array of legally significant «Documento Electorale №4, Acta Final Cierre y Escrutinios » (Acta №4, further in the text as the Act).

4.2. Goals and Objectives of the System

The goals of creating the System are:

- elimination of errors and falsifications associated with uncontrolled copying and distribution of hard copies of the Acts;
- providing citizens of the Republic of Guatemala with up-to-date and accurate information on the course and results of voting;
- creation of tools for public control and audit of the public administration of the electoral system of the Republic of Guatemala (in terms of implementation and support of the electoral process) by digitalizing the process of recording Acts and creating a trusted environment that excludes manipulations and the possibility of incorrect interpretation of intermediate and final voting results.

Objectives that need to be achieved to meet the set goals:

- develop a mobile application for creating a digital copy of the Act;
- create the possibility of comparing a paper document of the Act and a digital copy of the Act, approval of a digital copy of the Act by authorized participants in the voting process and saving a digital copy of the Act in the blockchain;
- implement blockchain technology and smart contracts to provide a trusted environment for public voting auditing;
- implement an independent counting of votes based on the processing of digital copies of Acts;
- implement the possibility of recounting the voting results, if necessary (for example, when the TSE decides to recount);
- implement functions of online provision of preliminary voting results from voting centers in near real time;
- implement for users the functionality of verifying the originals of the Acts published on the official portal of the TSE, with their digital copies certified at the voting center;
- implement for users the functionality of analytics and statistics based on voting results in various aspects.

4.3. System Capabilities

The system capabilities are divided into functional (ensuring the implementation of business requirements) and non-functional (service, ensuring the implementation of non-functional requirements). The list of functionalities is due to the detailing of the tasks facing the system.

Non-functional capabilities provide such indicators of system quality as maintainability, mobility, and others.

4.3.1. System Functionality

The functional system capabilities:

- calculation and presentation of voting results, including:
  - creation of a digital copy of the Act;
  - comparison of a paper document of the Act and a digital copy of the Act, approval of a digital copy of the Act by authorized participants in the voting process and saving a digital copy of the Act in the blockchain;
  - providing a trusted environment for public voting auditing by blockchain;
  - independent counting of votes based on the processing of digital copies of Acts;
  - the ability to recount the voting results if necessary (for example, when the Supreme Court decides to recount);
  - publication on the Internet of preliminary results from voting centers, as the signed Acts are issued and their digital copies are created, in near real-time, in the period until the publication of the official election;
- the ability to quickly and easily verify the originals of Acts published on the official portal of the Supreme Court for Elections (TSE), with their digital copies certified at the polling station, including:
- the ability to quickly and easily receive analytical and statistical reports on the results of the voting in various aspects (by the distribution of votes among political parties, by polling station, by the department, by country, etc.).

4.3.2. Service (supporting) Capabilities

The non-functional system capabilities:

- ensuring the normal functioning of the System;
- providing support for the System users;
- providing mobile access to the System;
- monitoring the normal functioning of the on-chain components of the System.

4.4. General Vision of the System

This section sets out a general vision of the future System, which is based on a list of the required functionality. The vision is required to understand whether the System is realizable with the necessary and sufficient set of capabilities using modern information technologies.

The first step in understanding whether the System is realizable with the specified set of capabilities is to develop a detailed scenario for using the System in practice, in the process of voting, registration of voting results at polling stations, and subsequent public audit of its results.

4.4.1. Context of the situation and conditions for working with the System

Over 20,000 Voting Tables are located across the country in approximately 1,000 Voting Centers in 340 Municipal Bodies spread across 23 Districts. The results from the voting tables are consolidated in the voting centers, then in the municipalities, then in the districts, and the districts are already collecting totals for the country and transmitting to the national level at the Tribunal Supremo Electoral (TSE).

Each voting table has a minimum of three and a maximum of five volunteers. They are accompanied by observer-witnesses (Fiscal) from any party that wishes to monitor their activities and records any disagreements over the vote.

Several hundred citizens are assigned to each table based on geographic proximity to their registered voting address. On election day, each citizen authenticates at his voting table and receives a paper ballot (or several ballots, depending on the number of elections held on that day).

At the end of voting day, voting centers are closed, and only officially authorized persons are allowed to count. All ballots are counted in front of the witnesses (Fiscals), which makes it possible to register objections in case of disagreement between volunteers and/or witnesses to vote on each ballot.

Arising problems (disagreements) are transferred to a higher authority for consideration only if the sum of these disagreements can affect the election results.

The voting results are calculated for each party, and the consolidated result is recorded manually in the consolidated act (Acta №4) in two copies.

All volunteers and witnesses sign the document only after reaching an agreement between them. This consensus algorithm is almost impossible to crack, given the physical presence of representatives of opposing political forces at the discussion.

Acta № 4 at this moment becomes the only legally recognized document on the results of voting at a specific voting table of the corresponding voting center.

The main copy of Acta №4 (called a duplicate) is had over by a volunteer to one of the temporary employees hired by TSE's IT department and assigned to a specific voting center.

At this point, it becomes possible to implement three options for improving the public audit of voting results.

4.4.1.1. Option 1 (preliminary) based on Acta №4 JPG files hosted in TSE database

An employee of the TSE IT department digitizes a paper copy of Acta №4 using a scanner and a laptop, forming a JPG file, and transfers this file via an Internet modem to the TSE IT department for placement in the database of preliminary voting results.

All JPG files with the results listed, after going through several private databases created by private contractors of TSE IT department, are eventually published on the TSE website in the preliminary results section.

By means of the System, these JPG files can be compared with files placed on the blockchain, as implemented in # Fiscal_Digital's proposal to the Guatemalan Elections Authority (TSE), https://www.gbaglobal.org/fiscal_digital_2020/, section «Our proposal for the region».

Quote: «Include a purpose built IOS or Android device at each voting table to photograph ORIGINAL summary table documents (Acta №4) as soon as they are created by the voting table volunteers themselves. The local app on the device will upload the JPGs to as many blockchains as possible, including the hash of a JSON that includes geolocation, timestamp, table ID and unique device ID (IMEI), thereby replacing dozens of handwritten, carbon paper certifications with a single digital blockchain certification.

Re-design voting table results documents (Acta №4) for optimal OCR performance via automatic systems as well as crowdsourced efforts. Ensuring that machine OCR is able to produce preliminary results eliminates the need for human-generated results for informative purposes with no legal impact on official results. Machines generate the public preliminary results; human volunteers check their work via #Fiscal_Digital and other similar civilian audits.

Re-define IT department's role as the implementer of blockchain certifications and OCR technology as efficiently and transparently as possible instead of contracting thousands of temporary workers and other third parties». End of quote.

Option 1 does not require electoral law changes (Congressional intervention) but requires approval from the TSE or the TSE Commission for the Renewal and Modernization of the Electoral System of the Republic of Guatemala (CAME).

No such approval was received for the Fiscal_Digital initiative in 2020.

4.4.1.2. Option 2 (optimal) with the transformation of the paper Acta №4 by the employees of the TSE IT department into a data model for the blockchain with the possibility of analytical and statistical analysis

This option also does not require electoral law changes (Congressional intervention) but requires approval from TSE or the TSE Commission for the Renewal and Modernization of the Electoral System of the Republic of Guatemala (CAME).

Permission from TSE or CAME is required for temporary employees of the TSE IT department to digitize paper Acta No. 4 using the Digital Voting Audit App and place it on the blockchain instead of digitizing paper Acta No. 4 using a scanner into JPG format.

In this case, the public audit of voting will be much more effective, and the preliminary voting results will be accurate, transparent, easily accessible to the public and officials, without the possibility of falsification of any kind.

This result is based on the fact that the «primary source of truth» is the legally approved paper, but correctly digitized Acta No. 4, which:

- has a developed and recorded consensus between officials (volunteers and fiscal witnesses);
- is placed by an official TSE IT employee directly into the trusted blockchain environment, receiving a cryptographic guarantee of authenticity;
- is the primary source of guaranteed data that is not converted into a JPG image, understood only by people, but into a machine-readable data model with the possibility of any processing by computers (analytics, statistics).

4.4.1.3. Option 3 (duplicate) with the formation of two streams of digital copies of Acta №4 - official and public

This option also does not require electoral law changes (Congressional intervention), but requires permission from TSE or CAME for volunteers to digitize paper Acta # 4 using the Digital Voting Audit App and put it on the blockchain.

At the same time, an employee of the TSE IT department digitizes the paper copy of Acta No. 4 as before - using a scanner and a laptop, forming a JPG file, and transfers this file via an

Internet modem to the TSE IT department for placement in the database of preliminary voting results.

Thus, there are two streams of digital documents - official and public, which can be subjected to comparison and independent verification for inconsistencies in the results of the vote count.

In this case, the public audit of voting is based on the "trust but verify" metaphor to the official voting results.

In today's conditions, it seems expedient to implement the System according to option 2.

The technical component of the project does not significantly depend on the option chosen.

4.4.2. Scenario of using the System (Use case) according to the optimal option 2

1. All employees of the TSE IT department working at the voting center install the Digital Voting Audit App mobile application (hereinafter referred to as the Application) on their smartphones and authorize it by entering a seed phrase issued by the administrator of the Digital Voting Audit Guatemala System.
2. Each officially signed Act at each voting table is digitized by the mobile application Digital Voting Audit App installed on the smartphone of the TSE IT department employee working at the voting table; thereby creating a machine-readable digital copy of each Act; at the same time, digitization of Acta No. 4 using a scanner into JPG format is not performed.
3. A digital copy of the Act is certified using the Application, by an authorized employee of the TSE IT department.
4. After certification, a digital copy of the Act is placed in the Digital Voting Audit Guatemala blockchain system, developed based on Free TON (hereinafter referred to as the System), with the guarantee of the invariability of each digital copy and the impossibility of making changes to it during the elections in the regular mode (in case of deviations from normal mode - see below item 7).
5. Online access to digital copies of the Act is provided to all users of the System through the Application or the web version of the System.
6. All instances of digital copies of the Act after they have been entered into the System, during the further course of the elections, are not related to the electoral legislation of the Republic of Guatemala and serve the System's purpose specified in section 4.1.
7. In the event of deviations from the regular mode[1] of holding elections, the System administrator launches an appropriate procedure[2] aimed at restoring the compliance of digital copies of the Act in the System with their modified paper originals.
8. The System user has the ability through the mobile application or the web-version of the System:

[1] for example, in the case of a TSE decision to recount votes in some precincts, or other legally significant action during an election that affects the data contained in one or more copies of the Act

[2] stipulated by the rules of operation of the System and ensuring the unconditional identity of the original of the Act and its digital copy

8.1. receive preliminary results from voting tables, as the signed Acts are issued and their electronic copies are created, in near real-time, in the period until the publication of the official election results;

8.2. check the originals of the Acts published on the official TSE portal with their digital copies;

8.3. request and receive analytical and statistical reports on the results of the voting in various aspects (on the distribution of votes between political parties, by voting center, by the department, by country, etc.);

8.4. publish on any Internet resources (websites, social networks, channels, etc.) any links to the results of their analytical and statistical queries to the System.

9. Upon completion of the elections, the public and the expert community of the Republic of Guatemala, using the System, analyzes the conduct of elections, evaluates the useful effect of the System's operation, and analyzes user requests to the System. The results are published in the public domain.

10. Based on these results, recommendations are developed:

    10.1. to improve electoral procedures and amend legislation on elections in the Republic of Guatemala;

    10.2. to improve the System and the practice of its application;

    10.3. on the dissemination of the advanced electoral experience of the Republic of Guatemala to other countries of Central and South America.

This scenario is the basis for the selection of the necessary and sufficient set of technologies and components of the System.

4.4.3. Architectural Approach

The vision of the System is that its objectives and capabilities can be effectively implemented technologically (and further developed) only when using a holistic architectural approach indicated in Figure 1. General Architecture.

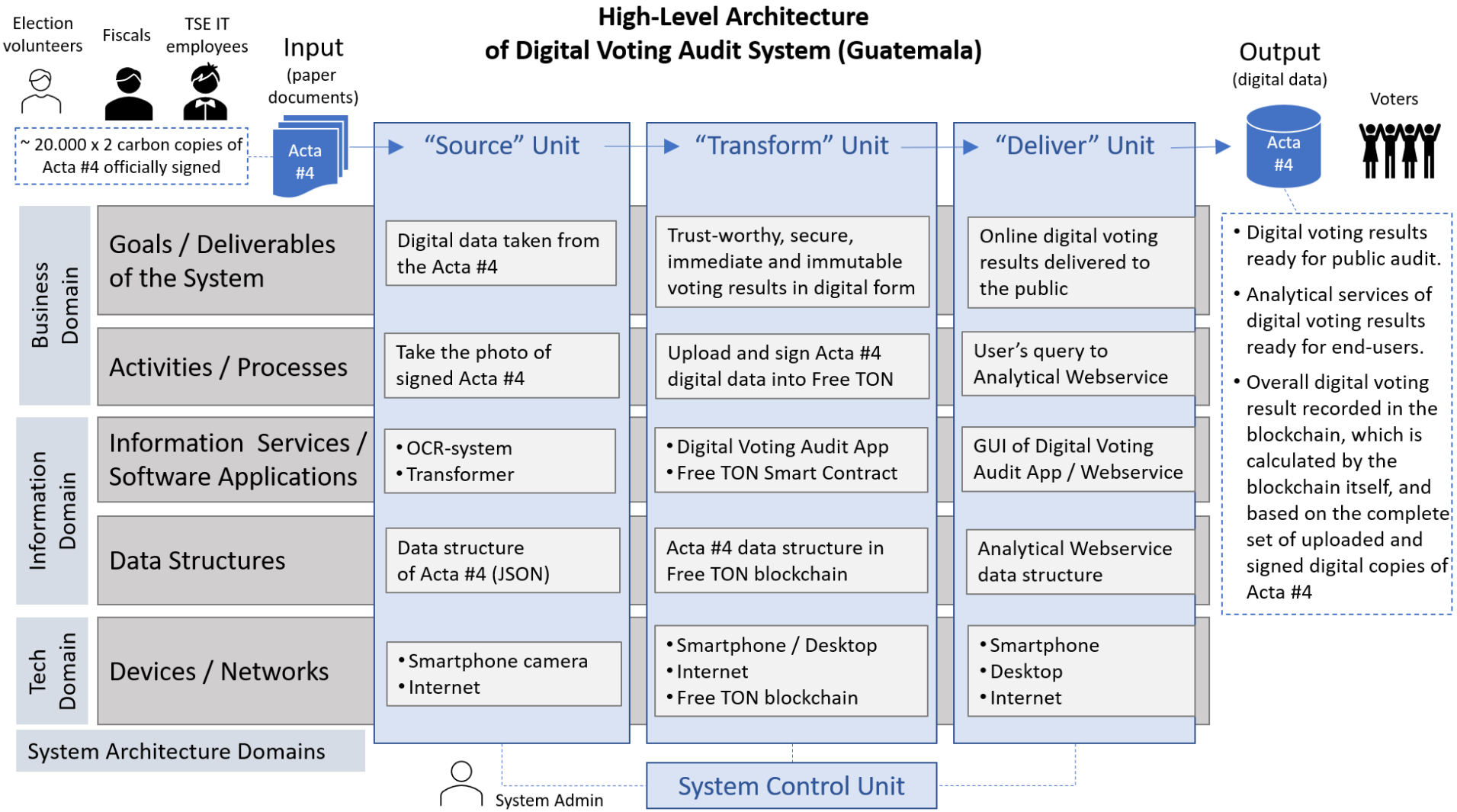

Figure 1. General Architecture

Such an approach, covering in a single matrix all the necessary architectural domains (information system stratums) and the main system components that provide the main process with input and output, gives an integral picture of the goals and work processes, information services, data structures, technologies and the results obtained.

This framework does not allow for mistakes in the conceptual design of the System at the present stage and provides a convenient decomposition of system elements to the necessary and sufficient level - at the subsequent stages of the design and implementation of the System.

The concept of «information system stratum[3]» improves the well-known TOGAF approach and allows it to be used not only in the design of corporate information systems but also in the creation of large-scale systems at the national level, in this case, for a distributed online system for auditing election results in the Republic of Guatemala.

The order of the levels of stratification is determined as the complexity of the processed information increases from simple to complex, from simple hardware equipment signals to the goals of the organization's existence.

1. At the lowest level is the stratum of machine codes and hardware. These are signals, assembly instructions, data in the form of bits and bytes. In the present concept, this is Tech Domain: Devices / Networks.
2. The second stratum from the bottom is structured data, information models that describe the structure of information (for example, the ER-model «entity-relationship»), the data is of a transactional nature, located in databases (DB), in the management systems of these databases (DBMS), and in blockchains (distributed ledgers). In the present concept, this is Information Domain: Data Structures.
3. The third stratum - information services, for example in the form of software applications, containing business logic and providing the necessary functionality to the end-user of the system. In the present concept, this is Information Domain: Information Services.
4. The fourth stratum is the conduct of the current activities of the organization, the functions and work processes performed by people. In the present concept, this is Business Domain: Activities / Processes.
5. On the fifth stratum are the goals of the organization. This stratum is the resultant one, which answers the question: why are all the underlying stratums needed? In the present concept, this is Business Domain: Goals / Deliverables.

Thus, the proposed vision of the System:

- contains comprehensive improvements to the technology of public audit of voting results in the Republic of Guatemala, eliminating the main problems in this area

[3] R.Gimranov, I.Kholkin. Reinventing Information Systems. Theory and Practice. Appendix 1. Emergent Information System Stratification. https://www.elibrary.ru/item.asp?id=43145902

(reduced voter confidence in election results and high costs of conducting voting and its audit);

- relying on a scientifically based methodology for stratification of information systems, it offers a holistic effective approach to the implementation of the current project, and also indicates rational directions for the digital transformation of the electoral system of the Republic of Guatemala as a whole.

4.4.4. Justification of the Selected Set of Technologies

The selected set of technologies and architectural components is based on the following:

- such a complex ensures the implementation of the specified initial requirements and takes into account the existing limitations, meeting the requirements for improving the situation in the subject area specified in Section 3;
- since the proposed solution will not require changes in the electoral legislation, the goal is achieved according to the usual methodology for implementing an IT project without involving state authorities of the Republic of Guatemala;
- such a complex does not require significant capital investments and purchases of fixed assets and will be available for use by both the System participants and the general public since almost everyone has a smartphone with a camera and the Internet;
- the technological advantages of using blockchain in the field of voting are widely known and are indicated in the section «Assessment of Feasibility»;
- the ideological advantages of using the blockchain, namely the ability to achieve a decentralized consensus through a censorship-resistant protocol that does not transfer (personal) data to third parties.
- it is not required to create (which will lead to cost savings and reduce the time required to create the System) a special clone of the Free TON blockchain (fork), since to implement the requirements of decentralization, transparency, and openness during voting, it is enough to develop a complex of smart contracts; at the same time, smart contracts are initially an important part of the Free TON ideology, and smart contract development tools are organically built into the technology;
- during the operation of the System, Free TON tokens will be used as a means to ensure the operability of the System's functionality. Execution of any logic on-chain and storage of data on-chain will consume tokens that will be used as payment for the work of validators that support the blockchain network.

Thus, the proposed vision of the System:

- contains comprehensive improvements in the technology of public audit of voting results in the Republic of Guatemala, eliminating the main problems in this area (reduced voter confidence in the election results and high costs of conducting voting and its audit);
- relying on a scientifically based methodology for IT stratification, it offers a holistic effective approach to the implementation of the current project, and also indicates rational directions for the digital transformation of the entire electoral system of the Republic of Guatemala.

5. Architecture of the System

In accordance with Section 4.4.3 «Architectural Approach», the architecture of the System includes three domains - Business Architecture, Information Architecture, Technical Architecture.

5.1. Business Architecture

5.1.1. Business Processes

Enlarged, the main business process of the System consists of the following set of types of activities, which, among other things, include activities for processing negative scenarios and exceptions during the execution of the main business process:

1. Obtaining permission from TSE or CAME for TSE IT department employees to digitize paper Acta No. 4 using the Digital Voting Audit App mobile application.
2. Installing the Digital Voting Audit App on smartphones of TSE IT department employees working at the polling station.
3. Receipt of blockchain keys by TSE IT department employees working at the voting center (the employee becomes a key holder)
4. Transfer of the signed paper Acta No. 4 from the election volunteers to the employees of the TSE IT department.
5. Digitization of the key holder of paper Acta No. 4 by means of the Digital Voting Audit App (creating a machine-readable digital copy of Acta No. 4);
6. Certification by key holder of a digital copy of Acta No. 4.
7. Placing a certified digital copy of Acta No. 4 in the Digital Voting Audit Guatemala blockchain system based on Free TON (hereinafter referred to as the System).
8. Provision of access to a certified digital copy of Acta No. 4 to all users of the System.
9. In case of deviations from the regular mode of holding elections, the System administrator launches an appropriate procedure to restore the compliance of digital copies of Acta No. 4 located in the System with their modified paper originals.
10. The System user can access the System through a mobile application or web-version of the System.
11. Receipt of preliminary results from voting centers by the user of the System, as digital copies of Acta No. 4 are created.
12. Verification by the System user of Acta No. 4 originals published on the official TSE portal, with digital copies of Acta No. 4 in the System;
13. Formation by the user of the System of analytical and statistical reports on the results of voting in various aspects.
14. Publication on the Internet resources by the user of the System of the results of his analytical and statistical queries.
15. Analysis by the public and the expert community of the election results.
16. Assessment by the public and the expert community of the beneficial effect of the System. Analysis of user requests to the System.

17. Publication of analysis results in open access.
18. Information support for the development of recommendations:

    18.1. to improve electoral procedures and amend legislation on elections in the Republic of Guatemala;

    18.2. to improve the System and the practice of its usage;

    18.3. on the distribution of the advanced electoral experience of the Republic of Guatemala to other countries of Central and South America.

5.1.2. Role Model of the System

The role model and rules of access and administration within the System are built taking into account the specifics of the System's subject area and the proposed vision of the System.

It is assumed that the role model of the System will be incremental. This means that each user of the System will be assigned a primary role by default ("User"), and additional functionality will be available to the user after adding additional roles.

This section summarizes the key functions within the structural elements of the System for large user types:

1. User - the main role that is assigned to any user. User is a Citizen of the Republic of Guatemala or a person who is interested in elections in the Republic of Guatemala. By default, has access to the information functionality of the System;
2. Key Holder - a citizen of the Republic of Guatemala (for example, an observer at voting centers in Guatemala), a privileged user of the System. They can work with Acts and digital copies of Acts that are entered into the System.
3. Admin - an additional role that allows you to perform certain administrative functions within the System.
4. Support - an additional role that allows you to access the functionality of the Support & Content backend subsystem.

5.2. Information Architecture

5.2.1. Data flow of the main process

The following figure shows data flows and artifacts of the main business process of the System in relation to user roles and software components.

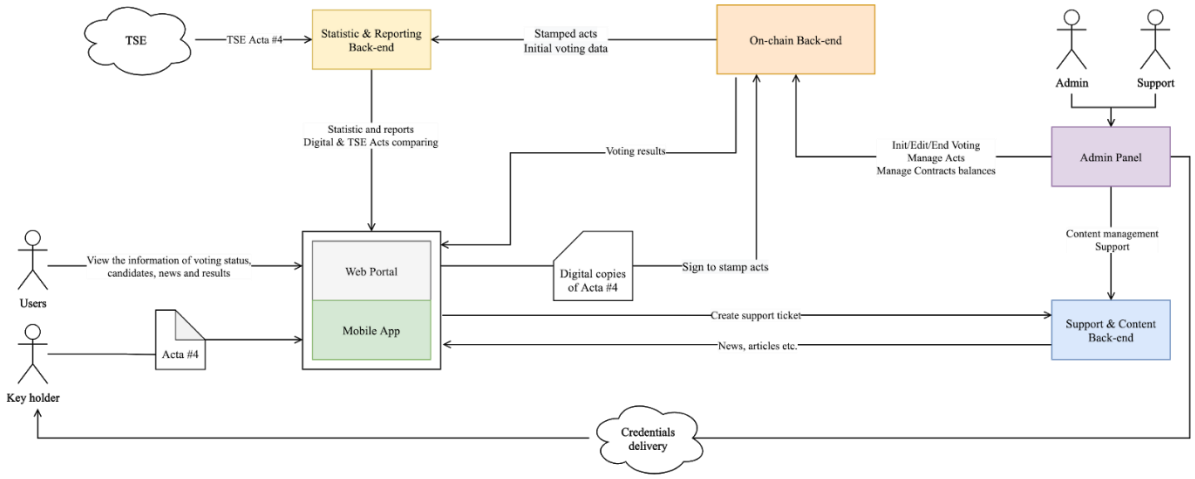

Figure 2 – Data flow and main artifacts

5.2.1.1. Creation of a voting

The following figure shows the sequence of actions of the System when creating a voting.

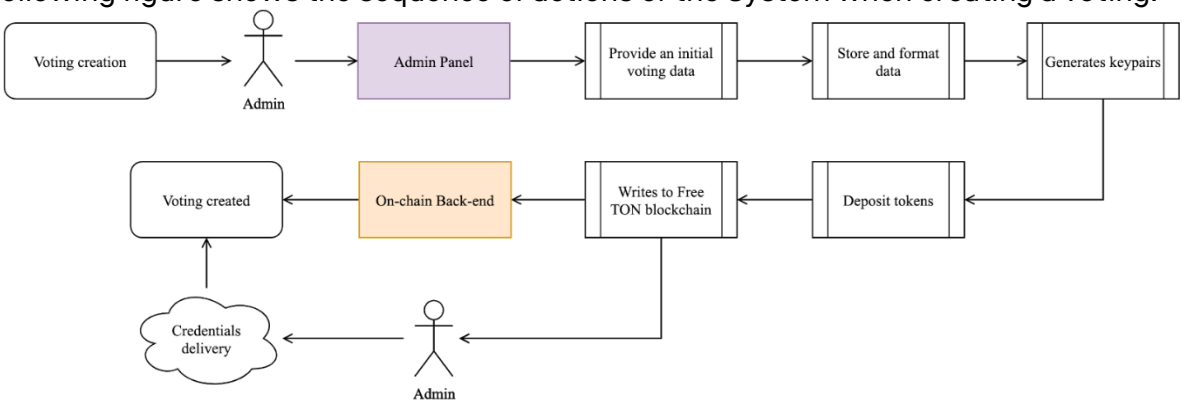

Figure 3 – Voting Creation Flow

Required artifacts:

- Information about voting (details are provided in section 5.2.4).
- Tokens to ensure the functioning of the System.

Main scenario:

1. The administrator goes to the Admin Panel.
2. Provides the necessary data to initiate voting.
3. The «Admin Panel» subsystem formats the entered data array for loading into the blockchain, creates a local backup.
4. Generates key pairs for Keyholders.
5. Awaiting the transfer of the number of tokens required to start voting.
6. After the receipt of tokens, the subsystem initiates voting in the blockchain.
7. Provides the Administrator with an array of Keyholders tied to Voting tables.
8. The administrator delivers keys for Key Holders.
9. Voting is created.

5.2.1.2. Downloading and signing a digital copy of the Act

The following figure shows the sequence of the System's actions when downloading and signing a digital copy of the Act.

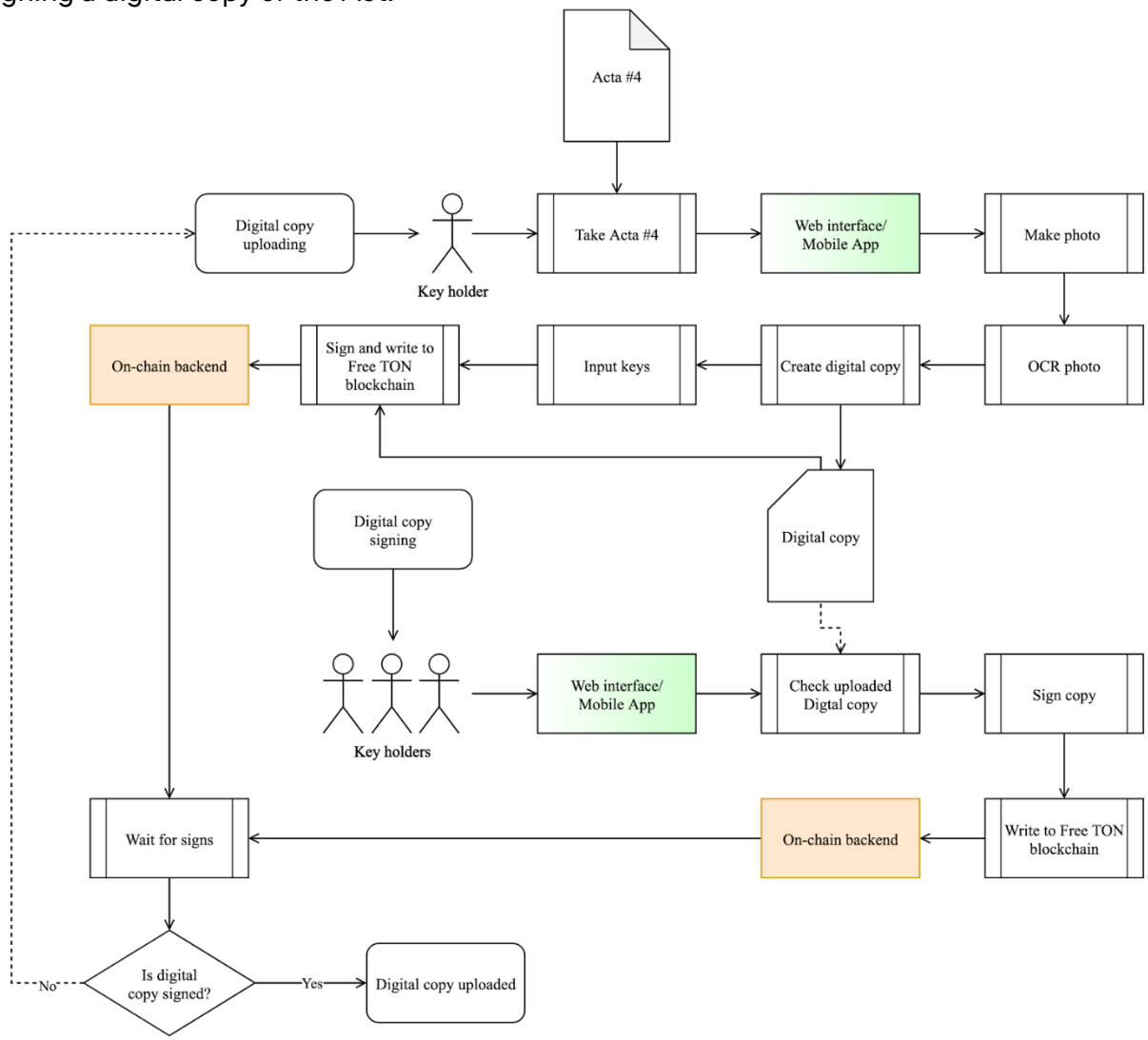

Figure 4 – Digital Copy Uploading and Signing

Required artifacts:

- Original Acta # 4.
- Keys for signing Acts.

Main scenario:

1. Key Holder receives the original Acta # 4.
2. Logs into MobileApp or Web Portal (hereinafter the Interface).
3. Takes a photo of the original Acta # 4.
4. The interface produces optical character recognition from a photograph. Formats the recognized text into the format required for recording, provides it for editing.
5. Key Holder confirms the correctness of the electronic copy. Introduces the key.
6. An electronic copy is recorded in the blockchain.

7. Subsystem «On-chain backend» is waiting for the signing of the rest of the Key Holders:
    a) Key Holders go to the interface;
    b) Key Holders review the uploaded digital copy of their Voting Table Act;
    c) Key Holders enter keys for signing;
    d) the interface writes signatures to the blockchain.
8. If a digital copy of the document was signed by 50% + 1 KeyHolder in the allotted time, the digital copy is recorded in the blockchain as a Stamped Act
9. If the digital copy was not signed by Keyholders within the allotted time, then this digital copy is canceled, you go to point 1.

5.2.2. System software components and tasks implementation

In the following table:

- the software components that make up the System are defined;
- the relationship between software components and the tasks of creating the System is determined.

Table 1 – connection of the software components of the System with the objectives of the System

		Digital Voting Audit (Guatemala) System					
		System Components					
		1	2	3	4	5	6
#	Objectives	MobileApp	Web Portal	Admin panel	Statistics & Reporting backend	On-chain backend	Support & Content backend
1	Development of a mobile application for creating a digital copy of Acts	+		+		+	
2	To compare Act and digital copies of the Act, approval of the digital copy of Act by authorized participants of the voting process and save a digital copy of the Act in the blockchain	+	+	+		+	
3	To implement blockchain technology and smart contracts to ensure a trusted environment public audit of the voting					+	
4	Implement independent counting of votes based on processing digital copies of Acts				+	+	
5	implement the possibility of recounting the voting results if necessary	+	+		+	+	+
6	Implement functions for online provision of preliminary voting results from voting centers in near-real-time mode	+	+		+		
7	Implement the functionality for users to verify the original Acts published on the official portal of the Supreme court of elections, Tribunal Supremo Electoral (TSE), with their certified digital copies at the voting center	+	+				+
8	Implement the functionality of analytics and statistics based on voting results in various sections for users				+		

The system is a combination of the following software components:

1. Subsystem MobileApp
2. Web Portal subsystem
3. Subsystem Admin panel
4. Subsystem Statistics & Reporting backend
5. Subsystem On-chain backend
6. Support & Content backend

Further, in the text, there is a brief description and basic characteristics of each subsystem of the System.

MobileApp

The subsystem is designed to interact with the users of the System and is a collection of applications for mobile devices. The subsystem consists of three modules with equivalent functionality:

1. iOS App
2. Android App
3. Windows Mobile App

MobileApp is the main interface for interaction with the System for category users (in detail, the roles and rights of users will be discussed in the section “Role model of the System):

1. Users
2. Key Holders

Below is the list are the theses concerning the basic functionality of the MobileApp subsystem:

- interface for creating a digital copy of the Act (with a manual filling of fields and using OCR);
- interface for editing a digital copy of the Act;
- user authorization interface;
- interface for recording a digital copy of an act in the blockchain;
- interface for access to the base of original Acts;
- user support interface;
- interface for viewing the news stream;
- interface for viewing reports.

Web Portal

Communication subsystem that is designed to interact with users. The functionality is similar to MobileApp, other technologies are used for its implementation. It is an alternative MobileApp way of interacting with System (Web) users.

The functionality of the Web Portal subsystem is similar to that of MobileApp:

- interface for creating a digital copy of the Act (with a manual filling of the fields and with downloading a scan of the Act);
- interface for editing a digital copy of the Act;
- user authorization interface;
- interface for recording a digital copy of an act in the blockchain;
- interface for access to the base of original Acts;
- user support interface;
- interface for viewing the news stream;
- interface for viewing reports.

Admin panel

This subsystem is intended for administration of the System, separate business logic, and integrations with external systems. Users of the Admins category have access to this subsystem.

The main functionality of the subsystem:

- maintaining reference books of the System
- interface for deploying smart contracts;
- interface for generating keys for privileged categories of users (Key Holders);
- interface for monitoring the balance of smart contracts;
- monitoring off-chain technical infrastructure and software;
- administration of the core backend (news feed, integrations).

Reporting & Statistics backend

This subsystem is designed to carry out calculations based on the data contained in the Acts. For primary calculations, it uses data stored in the blockchain. For the subsequent ones, calculations are made based on data stored off-chain. The API of this subsystem is used to get data in the interfaces for displaying data of user subsystems (MobileApp, Web Portal).

On-chain backend

The subsystem is designed to store and execute smart contract systems to ensure the functioning of the logic of the System's processes.

The main functionality of the subsystem (smart contract system):

- VotingRoot - implements the logic of working with votings;
- VotingData - contract for storing and counting voting results;
- ActsRegistry - contract-register of existing Acts;
- Act - smart contract of the act of the voting table;
- VotingResult - contract for counting and storing voting results.

The functionality of smart-contract systems is described in detail in the section «Description of the logic of functioning of smart contracts».

Support & Content backend

The subsystem is designed to support users and administer the System business logic related to the content provided to the System users in the following cases:

- incorrect operation of the System;
- incorrect or potentially incorrect information contained in the System;
- the need for changes in the business logic of the Content-related System.

In terms of user support functionality, it is an interface for 1st, 2nd, and expert support lines, which allows you to:

- register incidents and user calls;
- carry out classification, prioritization, escalation, and closure of incidents and user requests;
- register and support periodic and planned works;
- notify users in connection with user incidents and requests.

5.2.3. Architecture of Software Components

Statistics & Reporting Backend

The following figure shows the logical structure of the Statistics & Reporting Backend software component.

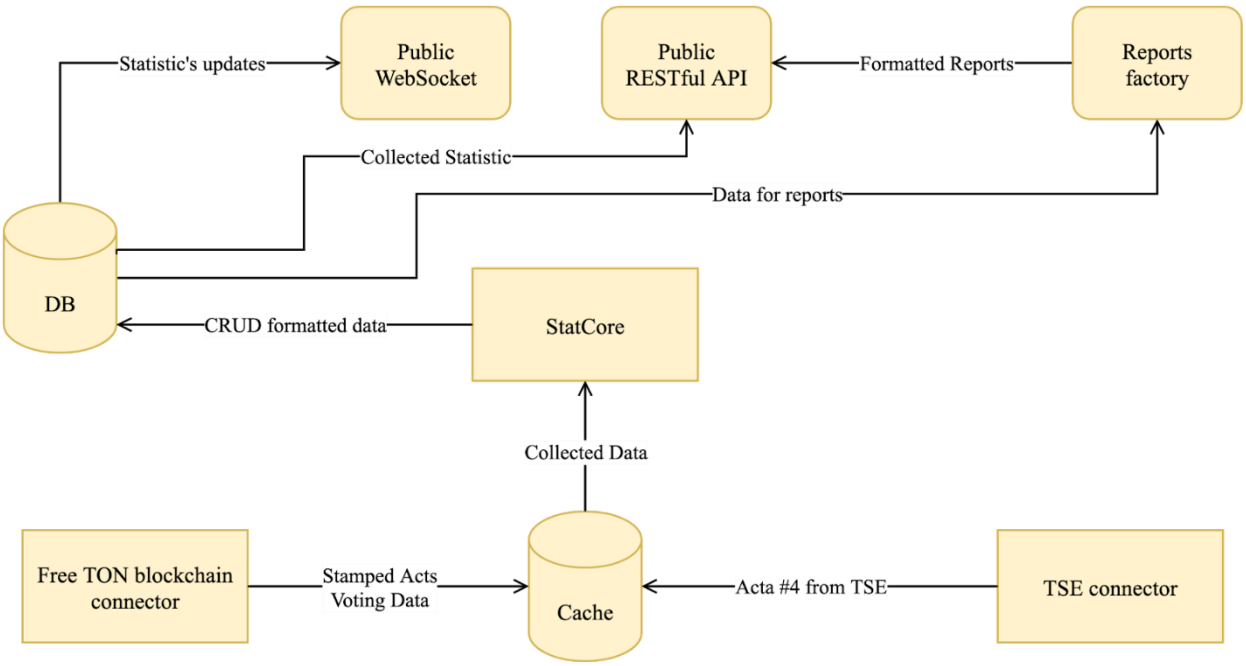

Figure 5 – Statictics & Reporting Backend Structure and Data Flow

- Free TON blockchain connector is a module for collecting, parsing, and caching up-to-date information about Stamped Acts from the Free TON blockchain network.
- TSE connector is a module for collecting parsing and caching up-to-date information about uploaded digital copies of Acta # 4 to the TSE website.
- Cache is a module for storing unstructured information for subsequent analysis and writing to long-term storage.
- DB is a long-term storage for the calculated information. It is used to issue to system interfaces and generate reports.
- StatCorp is the central module of the component that analyzes and transforms data into the required form for output to end interfaces.
- Reports factory – a module for generating reports from long-term storage data.

- Public RESTful API - the entry point to the component, provides methods for receiving information and reports.

Admin Panel

The following figure shows the logical structure of the Admin Panel software component.

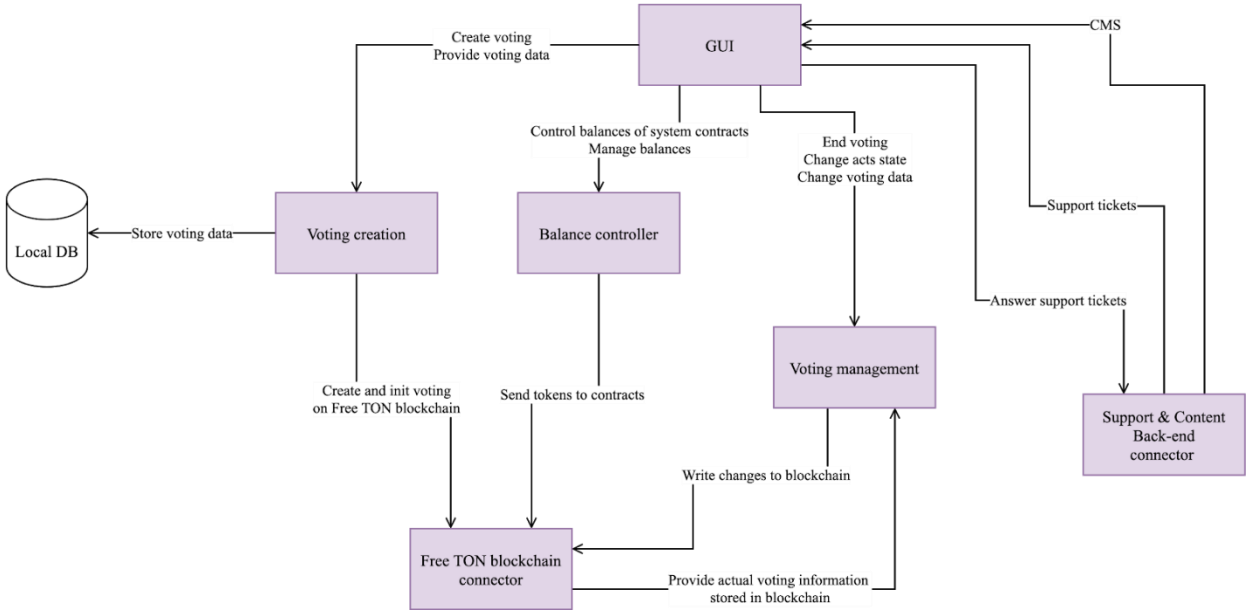

Figure 6 – Admin Panel Structure and Data Flow

- Free TON blockchain connector - a connector to the On-chain back-end subsystem. Serves for receiving and recording information in the Free TON blockchain
- Support & Content Back-end connector - connector to the Support & Content back-end subsystem. Receives and transfers system content, information for support specialists to the GUI.
- Voting management is a voting control module. Allows the Administrator to change information about voting, carry out recounts, complete voting.
- Balance controller - a module for monitoring system contract balances. Allows the administrator to monitor the system balances in real-time and, if necessary, change them.
- Voting creation - module for creating voting. Aggregates and backs up the data necessary to create a vote.
- Local DB - Local storage system for the entered data. The main function is to temporarily backup data until it is written to the blockchain.
- GUI - the graphical interface of the subsystem. Serves as the primary end-user entry point for the subsystem to interact with all other software components.

Support & Content backend

The following figure shows the logical structure of the Support & Content backend software component.

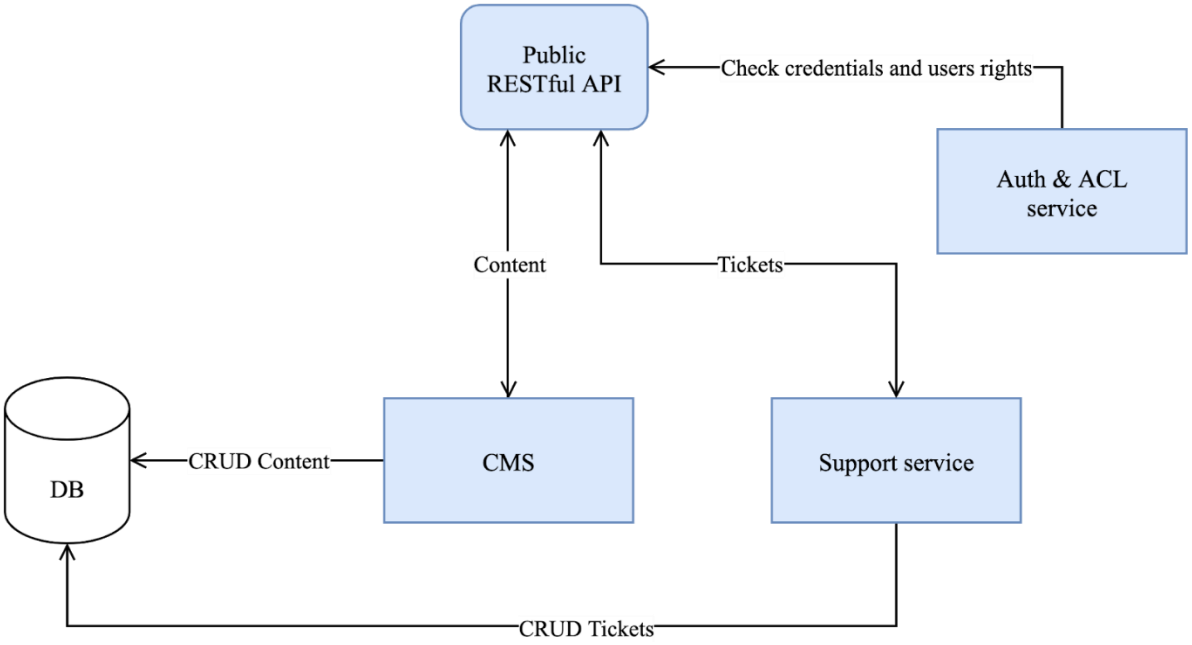

Figure 7 – Support & Content Structure and Data Flow

- Support service - a module that controls the flow of requests to the support system. Stores support requests and provides a communication channel between users and system support specialists.
- CMS is a module for managing system content. Carries out the necessary operations for recording, editing and issuing system content.
- Auth & ACL service - a module for authorization and user rights management. Issues authorization tokens. Provides access to the appropriate API routes based on user rights.
- DB - module for long-term storage of subsystem data.
- Publich RESTful API - the only entry point to the module, provides methods for interacting with the rest of the subsystem modules.

MobileApp and Web Portal

The following figure shows the logical structure of the MobileApp and Web Portal software components.

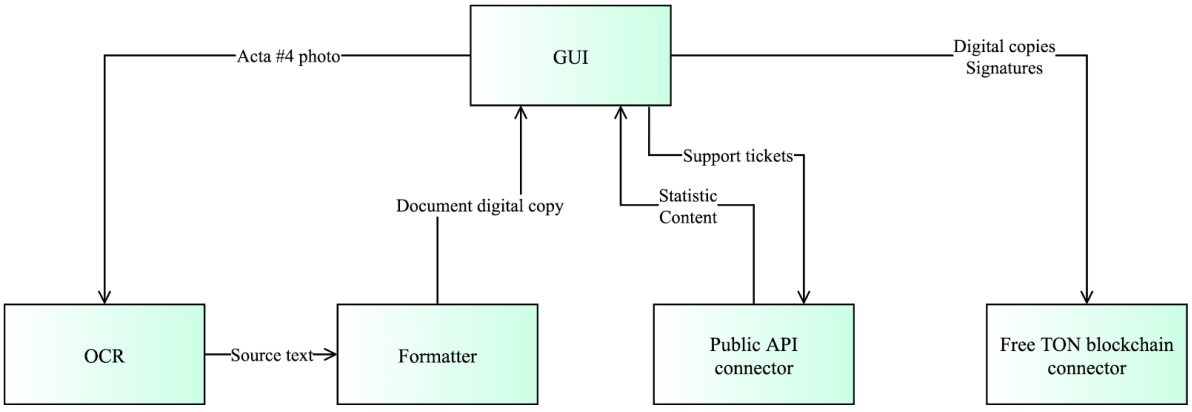

Figure 8 – MobileApp and Web Portal Structure and Data Flow

- GUI - the graphical interface of the subsystem. Serves as the primary end-user entry point for the subsystem to interact with the functionality of all modules in the subsystem.
- OCR is an optical character recognition module. Required to translate Acta # 4 photo into text format.
- Formatter is a module for converting text Acta # 4 into an acceptable format for loading into the blockchain. It also allows you to manually edit unrecognized / incorrectly recognized document elements.
- Public API connector - a connector to the public API of the system backends to receive data for displaying and submitting forms
- Free TON Blockchain connector - a connector to the Free TON blockchain for recording and signing digital copies of documents.

5.2.4. Description of the Logic of Functioning of the Smart Contract Cystem

The logic scheme of the On-chain backend software component is shown in the following figure.

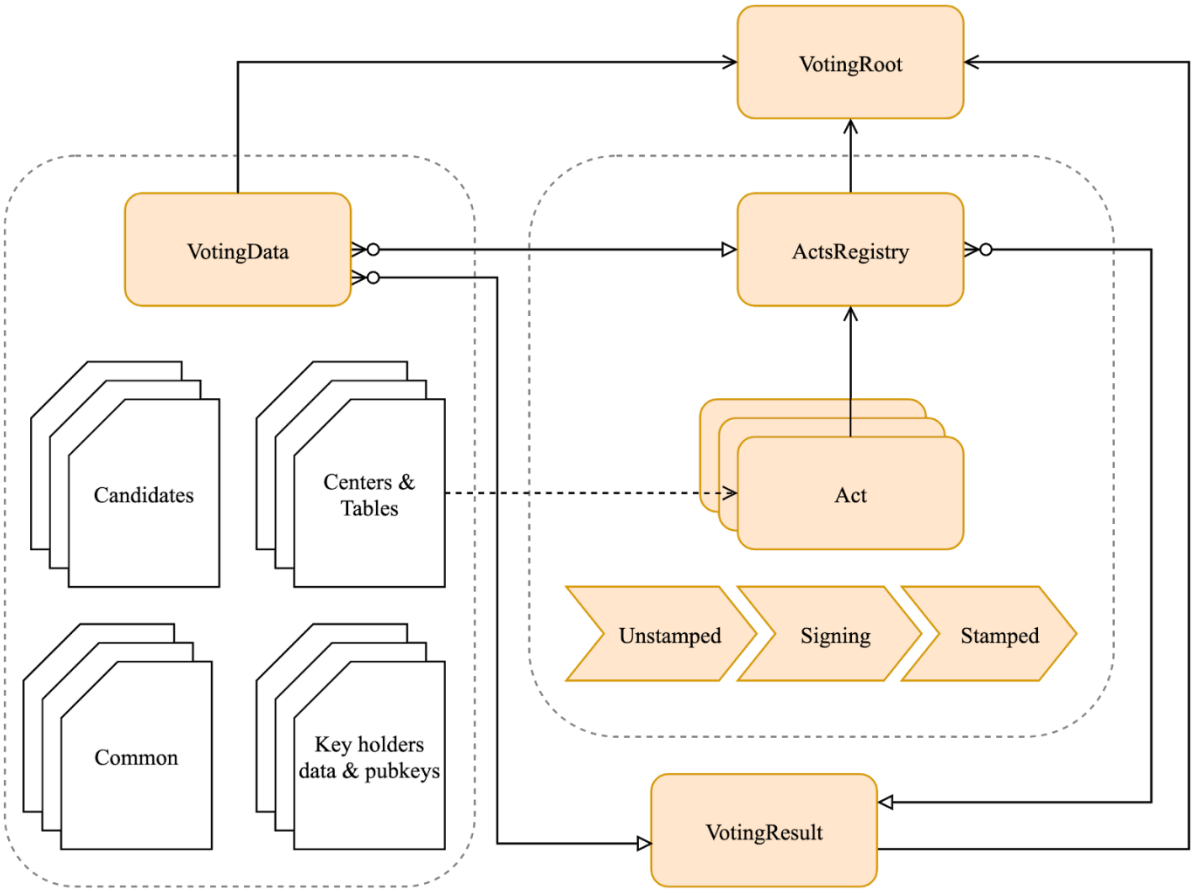

Figure 9 – On-chain backend Structure

The subsystem consists of the following contracts:

- VotingRoot;
- VotingData;
- ActsRegistry;
- Act;

- VotingResult.

VotingRoot

Subsystem central contract. Provides the main interface for interacting with the functionality of other contracts in the system. The contract provides access to the following operations:

- create a voting;
- end voting;
- receive information about voting;
- receive information about the voting results;
- get information about the current state of voting;
- upload and sign Acts.

VotingData

Smart contract needed to store voting data. It guarantees the persistence and integrity of data for reading both by the modules of this subsystem and by third-party systems and subsystems. Stores data such as:

- list of candidates;
- list of districts;
- list of voting centers;
- a list of Key holders that have keys for signing Acts;
- general information about the voting - title, dates, etc.

ActsRegistry

ActsRegistry is a contract-register of existing acts. It maps unique identifiers to the deployed Acts contracts and stores a ready-made list. Serves for simplified access to contracts of Acts by issued identifiers, and also ensures data integrity and persistence.

Act

Act is a smart contract of the voting table Act. Serves for storing and signing electronic copies of Acts.

The contract is associated with a specific voting table from VotingData. Keyholders of the assigned voting table, as well as the system administrator, have access to interact with the contract.

It has three states - *Stamped*, *Signing*, and *Unstamped*.

Initially, the contract is deployed in the *Unstamped* state and is waiting for a digital copy of the act to be loaded by one of the Key holders who have access to the contract. Then the contract goes into the *Signing* state and within N-minutes waits for transactions confirming the correctness of the downloaded electronic copy of the act. Keyholder who has uploaded the act is automatically considered to have signed it. Upon signing the 50% + 1 Keyholder deed of the plot, the contract goes into the *Stamped* state and is considered fixed. If the waiting time has expired, and the required number of signatures has not been

received, the contract clears the saved digital copy, goes into the *Unstamped* state, and waits for a new digital copy of the act to be loaded.

The system administrator can transfer the contract to the *Unstamped* state by deleting the fixed digital copy of the act at any time before the voting and counting of results are completely finished.

VotingResult

VotingResult is a contract for counting and storing voting results. The contract is started by the administrator at the end of the vote. When launched, the contract collects information from Stamped Acts, calculates the result, and saves statistics. Saved results cannot be changed.

Workflow

To start voting, the System Administrator must prepare the data for the VotingData contract described in the corresponding section, as well as the tokens required for the System to function. It is assumed that to simplify the initial placement of the On-chain backend in the blockchain, manage it and control balances, the “Admin Panel” software component will be used, which will perform all the necessary operations after receiving the data.

Distribution of keys to final Keyholders is performed outside the system.

Voting is considered completed when all acts are in the Stamped state, and the System Administrator has explicitly indicated the completion of voting.

5.3. Technical architecture

Below, for each of the software components and the System as a whole, there are descriptions of the complexity of software and hardware that can be used to implement the technical architecture of the System.

Common

- Container Orchestration System (Kubernetes)
- Containerization system (Docker)
- Web server (NGiNX)
- CI/CD tool (Jenkins)
- Version control system (Git)

Statistics & Reporting backend

- VDS (8 GB RAM, 4 CPUs, 80+ GB SSD storage)
- Linux (Ubuntu 18.04+ / Debian 9+)
- In-memory DB (Redis)
- DB (PostgreSQL)
- Backend programming language with analytics libraries (Python 3, Pandas)
- Backend programming language for RESTful API building (Node.js, loopback.js)
- TON SDK (ton-client-ts)

Statistics & Reporting Backend

- VDS (8 GB RAM, 4 CPUs, 80+ GB SSD storage)
- Support system (Naumen Service Desk or analog)
- Content Management System (Drupal or analog)
- Identity and Access management system (Keycloak)
- Compatible DB (My/PostgreSQL)

Admin Panel

- JS framework for SPA and environment (React, Redux, Webpack, TypeScript)
- Local DB (IndexedDB)
- TON SDK (@ton-client-ts/web, @ton-client-ts/node)

Mobile app and Web interface

- JS framework for SPA and environment (React, Redux, Webpack, TypeScript)
- Node.js OCR library (node-tesseract-ocr)
- Library for building cross-platform application (Electron.js)
- TON SDK (@ton-client-ts/node)

On-chain backend

- TON Smart-contract programming language (Solidity)
- Free TON blockchain
- tonos-cli
- Smart-contracts testing environment (Jest, @ton-client-ts/node)

6. Assessment of the System Feasibility and the Main Phases of Implementation

6.1. SWOT-analysis of Feasibility

Assessment of the feasibility of the project at this stage is based primarily on the SWOT analysis, which consists of identifying the factors of the internal and external environment and dividing them into four categories:

1. Strengths
2. Weaknesses
3. Opportunities
4. Threats

Strengths and weaknesses are factors of the internal environment of the object of SWOT analysis (that is, what the object itself is able to influence).

The object of SWOT analysis is the Digital Voting Audit Guatemala System for a public audit of voting results based on data from digital copies of paper Acta No. 4, stored in the Free TON blockchain.

Opportunities and threats are factors of the external environment (that is, those that can affect the object from the outside and that is not controlled by the object itself).

The external environment of the SWOT analysis is the electoral system of the Republic of Guatemala, including the subject area “Civil (public) audit of election results”.

At this stage of the project (conceptual design), the use of SWOT analysis is due to:

1. the universality of the method; it is applicable in various spheres of politics, economics, and management, including the electoral system of the state; the method can be applied to a research object of any level (document, voting center, region, country);
2. flexibility of the method; he has a free choice of the analyzed elements depending on the goals set (for example, you can analyze the electoral system only from the point of view of auditing the voting results, or from the point of view of improving the system as a whole);
3. the ability to use both for a quick assessment of the situation, and for strategic planning for a long period.
4. absence of requirements for special knowledge and narrow-profile education - for example, knowledge of the intricacies of the electoral legislation of the Republic of Guatemala;
5. correspondence of the objectives of this stage of the project to the possibilities of SWOT analysis and the competencies of specialists in the conceptual design of the System.

SWOT analysis at the conceptual design stage:

1. identifies only general factors affecting the situation; specific measures to achieve the set goals will have to be developed in subsequent stages.

2. lists the factors without dividing them into major and minor, without a detailed analysis of the relationship between them.
3. forms a static picture of as-is, without its evolution in time.
4. presents results in the form of a qualitative rather than quantitative description.

Each category is discussed separately and how they are combined in the SWOT matrix.

6.1.1. Strengths

The strengths of the proposed System are:

1. providing technological means to achieve the set goals:
    a) elimination of errors and falsifications associated with uncontrolled copying and distribution of paper copies of Acta No. 4;
    b) providing citizens of the Republic of Guatemala with up-to-date and accurate information on the course and results of voting;
    c) provision of tools for public control and audit of public administration activities (in terms of implementation and support of the electoral process) by digitizing the accounting process Acta No. 4 and creating a trusted environment that excludes manipulations and incorrect interpretation of intermediate and final voting results.
2. Benefits for public audit during digitalization Acta No. 4:
    a) paper copies of Acta # 4 provide consensus between civil volunteers and political party witnesses (Fiscals), and the strong cryptographically secure digitization of Acta # 4 reinforces this consensus by publishing the results and ensuring the credibility of each Act;
    b) placing Acta digital model # 4 directly in an immutable and publicly accessible format in the trusted blockchain environment ensures that the data of each Act cannot be falsified at subsequent stages of the electoral procedure;
    c) Acta # 4 digital model used for automatic generation of preliminary voting results eliminates the need to inform the press and the public “manually” without any legal consequences for the official results;
    d) all mediators become unnecessary, and thus any possibility of altering the election results will be eliminated;
    e) significant savings in hiring thousands of temporary staff will be saved, and millions of paper copies will not need to be printed;
    f) the unconditional integrity of information is ensured, and the speed of its provision to the public will be close to real-time;
    g) any third-party auditor will be able to confirm the results within a few hours with minimal cost;
    h) the opportunity for voters to participate in the voting audit directly from their laptop or smartphone, while significantly expanding the circle of persons involved in the audit;
3. Additional advantages when using the System in other spheres of public life:

a) no need to collect all interested persons in a certain place and at a certain time to make decisions on daily issues; people could get the opportunity to take part in public life by voting online when it is convenient for them and in a way that suits them;

b) the ability to compare decisions taken by different bodies or jurisdictions, to compare them with the results of past local votes; all the details of social activities can also be available to everyone; each participant can check both his own vote and make sure that the votes of other participants are recorded accurately.

6.1.2. Weaknesses

The most significant weaknesses of the System:

1. Excessive transparency of the blockchain. If the voting results are recorded on the blockchain in an unencrypted form, they are distributed to all users, intermediate results become available, which is contrary to the law and is misleading.
2. Blockchain technology is not clear to the average voter. It is necessary to show voters the transparency and power of attorney of the System when calculating the voting results based on data from digital copies of paper Acta No. 4 stored in the blockchain. In other words, in order to maintain confidence in the system, voters need proof of the correspondence of the data specified in the paper (agreed by volunteers and fiscals) documents Acta No. 4, and data in their digital copies placed on the blockchain.
3. The possibility of hacking the System (for example, if the size of the keys for encryption is less than 256 bits, then it is possible not only to hack the blockchain but also to monitor the course of elections in real-time; you can recover all the secret keys in a short period of time)[4].
4. If the system used for electronic voting is implemented as a closed one (corporate blockchain, without external interaction), then it will not be possible to conduct its independent audit, there will be no service for checking votes by voters; at the same time, it will be possible to verify the results only through the courts - then TSE, in theory, will agree to give access to the original blockchain with a key to decrypt data in a digital copy of Acta No. 4.
5. Hardware failures on the servers of the System are possible, stopping or delaying access to digital copies of Acta No. 4 in the blockchain; you will need to contact each of the voters who have difficulties with the audit, for example, a call from a call center, a push notification in your personal account, an e-mail or SMS message, so that the voters, after notification, return to the System and continue the audit.
6. For the uninterrupted operation of the System, it is necessary to exclude haste in development and implementation, as well as the use of low-quality hardware.
7. In the case of a serious intention of counterfeiters who have large funds for bribery, forgery in electronic voting can be carefully hidden in the program code - regardless of whether the blockchain is used or not.

[4] https://forklog.com/eto-ne-blokchejn-pochemu-sistema-golosovaniya-v-moskve-dala-sboj-i-primenima-li-ona-voobshhe-dlya-vyborov/

It is obvious that the functionality of the System based on only one blockchain is not enough - a complex of different technologies, applications, and processes is needed.

6.1.3. Opportunities

Opportunities are factors of the external environment (that is, those that can affect the System from the outside and that is not controlled by the System itself).

The external environment containing the possibilities for the implementation and development of the System is the electoral system of the Republic of Guatemala that has developed by that time.

The most significant opportunities for the implementation and development of the System:

1. The presence in the electoral system of the role function «Fiscal» - an observer or witness of the electoral process, who is responsible for keeping the electoral system under control. Fiscals protect the integrity of this system and maintain the confidence of voters in it. In fact, fiscal cannot interfere with the process, but only observe. But if a fiscal detects a problem in the process he is observing and realizes that it can be technically solved within the framework of the law, he must document the problem and then pursue it until it is resolved by the authorized body.
2. The role function «Fiscal» described above in paragraph 1 is in the current situation ready for digital transformation and can be implemented by means of IT. The #Fiscal_Digital application has been developed, which is actually an initial pilot project to test such a digital transformation; the experience of this project must be taken into account, eliminating the shortcomings of its concept and technical implementation (approval of the Fiscal_Digital initiative from TSE / CAME in 2020 was not received).
3. The civil society of the Republic of Guatemala is now convinced that reforms are needed in the electoral system, therefore, the implementation of the System that allows solving the problems of loss of voters' confidence in elections will be supported by civil society.
4. State authorities of the electoral system - the Tribunal Supremo Electoral (TSE), including the TSE's Commission for the Update and Modernization of the Guatemalan Election System (CAME) - are objectively interested in finding a solution that:
    a) allow to remove the negative attitude of the citizens of the Republic of Guatemala to the existing situation, exclude public protests;
    b) effectively improve the functioning of the electoral system;
    c) rebuild TSE's reputation damaged during the 2019 elections;
    d) will become a determining factor in strengthening the position of TSE in the country's government;
    e) will provide an opportunity to present the country's leadership with a significant positive result of its activities.

Independent democratic elections are the institution of social order for which blockchain technology is best suited; for example, the manifesto of the creators of bitcoin practically duplicates the provisions on elections laid down in the constitutions of developed democracies; therefore, blockchain technology, one way or another, sooner or later, will be

introduced into the electoral process; it is required to approach this in a state manner - thoroughly, deliberately and seriously.

6.1.4. Threats

Threats are factors of the external environment (that is, those that can affect the System from the outside and that at the same time are not controlled by the System itself).

The external environment containing potential threats to the System is the electoral system of the Republic of Guatemala that was established at that time.

A preliminary identified list of such threats for the implementation of the System:

1. Elections are a very responsible process, as a result of which legitimacy and trust in the authorities are born. Therefore, there is an opinion that:
    a) There can be nothing better than paper ballots, transparent ballot boxes, and the publicity of independent commissions - that is, no IT systems are needed for elections at all.
    b) blockchain is more a PR and attention grabber than a really new approach to organizing a voting system;
    c) blockchain is not a toy, it is a serious intellectual work, which today only a few professionals around the world are capable of, the names of most of them are known, and we have no data that any of them were involved in this project.
2. Experts may not understand what specific technical algorithm the System is built, what know-how was used (if used) - such information is indicated in the project documentation, which should be available.
3. The use of blockchain technology in the mass segment, that is, outside the environment of IT specialists, requires serious cultural training; training of electoral staff, volunteers, observers, information support of citizens; clarification of the principles of decentralization and conditional anonymity should play an important role in this - without understanding such basic things and reaching agreements “on the shore”, one should not begin the technical implementation of the System.

The effectiveness of identifying explicit or latent threats can be enhanced by using the Anticipatory Failure Determination method, which is based on the question «What should be done to cause maximum damage to the System, disable it or stop its implementation?». In fact, it is necessary to «come up with a sabotage» against the System, and then check what of what was invented has already been implemented in one way or another in the existing situation (that is, identify the explicit and hidden resources in the environment that ensure the implementation of potential threats).

6.1.5. SWOT- matrix

Table 2 – SWOT Matrix

	Opportunities	Threats
Strengths	What strengths of the System must be used in order to get a return on opportunities in the external environment	What strengths of the System should be used to eliminate possible threats
Weaknesses	Due to what opportunities available in the external environment, the System will be able to overcome the existing weaknesses	What weaknesses does the System need to get rid of in order to prevent possible threats?

Strengths - Opportunities

To benefit from the identified opportunities in the electoral system of the Republic of Guatemala, the following strengths of the System must be exploited:

1. The System provides for the technological implementation on the blockchain of the fundamental role function «Fiscal», which is already ready for digital transformation.
2. The System provides an IT solution that is a real step towards electoral reforms supported by the civil society of the Republic of Guatemala.
3. The System provides an IT solution in which the State authorities of the electoral system of the Republic of Guatemala are objectively interested.
4. The System is based on blockchain technology, which is best suited for use in the field of independent democratic elections and will be introduced into the electoral process - now or later.

Strengths - Threats

To eliminate possible threats, it is necessary to use the following strengths of the System:

1. The System is able to prove in practice that with a proper design, architectural and ideological approach, negative and skeptical opinions that exist in the public mind about the shortcomings of the blockchain will be eliminated.
2. The project team of the System will proactively inform the expert community of the Republic of Guatemala, which may not understand what specific technical algorithm the System is based on, what know-how was used, etc.
3. The project team of the System will proactively provide training for electoral staff, volunteers, observers, information support for citizens of the Republic of Guatemala in order to introduce a culture of decentralized technologies.

Weaknesses – Opportunities

The system will be able to overcome the existing weaknesses due to the following opportunities available in the electoral system of the Republic of Guatemala:

1. There is an expressed desire in civil society to get reliable, understandable, easily accessible from familiar devices such as a smartphone, means of checking the voting results; the system should and can provide such means so that they can be quickly tested in practice.
2. The project team of the System, due to its professionalism, is able to foresee possible attacks of falsifiers of voting and build an appropriate information security architecture; this approach will clearly be supported by both the public and TSE.
3. The System initially contains an integrated, holistic architectural approach that excludes focusing only on a single blockchain technology; the system's project team has developed an optimal systematic, balanced ideology and implementation strategy, taking into account the interests of the various parties involved in the elections; this approach will be purposefully promoted in Guatemalan society to garner support from organizations and individuals interested in improving the electoral system.

Weaknesses - Threats

To prevent possible threats, the following weaknesses of the System will be minimized:

1. Conducting a public audit of voting requires very strict security standards - after all, the temptation to falsify is too great and the risk of large-scale manipulation is quite high; Therefore, the System should not operate in a “black box” mode - the audit process should be clear and transparent for all participants, at any time there should be a possibility to monitor the process and check the results.
2. The system will be implemented using a public blockchain (it will not be closed and centralized, it will exclude the possibility of manipulation).
3. Hardware failures in the System will be minimized due to the distributed decentralized technological nature of the blockchain.

During the development and implementation of the System, an architectural and design approach that has proven its effectiveness will be used, eliminating haste and «overlaps».

6.2. Main phases of implementation

6.2.1. First phase (this concept)

At this phase, a public voting audit is implemented based on a digital copy of Acta No. 4, a quick digital presentation of the results to the public, with analytic capabilities, without changing the legislation and voting procedures.

The System of this phase is described in the above sections of this concept.

6.2.2. Second phase

This phase envisages the creation of a digital blockchain voting platform, covering both the level of ballots and the level of the final consolidated Acta No. 4, using both paper and digital forms of these documents.

In this phase, the System:

1. can solve the problem of ensuring independent control regardless of the level and type of voting - whether it is the election of the president of the country or the election of the best teacher in a city school;
2. does not require changes in legislation (ideally, of course, they are needed), but the System can function for some time without it.
3. can be expanded to include in the coverage of the System the process of remote voting (for example, from home).

6.2.3. Third phase

This phase provides for the development of the functionality of the System to a fully digital online voting based on the Free TON blockchain, which requires necessary and sufficient changes in the electoral legislation of the Republic of Guatemala.

This kind of voting is really convenient and very effective, but it requires very strict security standards for every aspect of it.

The ideology of the Free TON blockchain is based on smart contracts, the execution of which is technologically decentralized so that the correct execution of each of the voting conditions is automatically checked by the network participants themselves - validators. In the digital electoral system of the Republic of Guatemala, validation will be carried out by the so-called trusted representatives - observers (Fiscal), candidate representatives, volunteer public people.

The protocol and digital voting regulations will be implemented in the smart contract environment. All the necessary tasks - online voting itself, checking ballots, counting votes, reaching consensus at the polling station when registering the results in the final consolidated act (Acta No. 4), consolidation of these acts by the levels of the electoral system will be automated and decentralized through smart contracts in the trusted blockchain environment.

There will be no «black box» where ballots are sent for the counting of votes, carried out in ways that are not transparent for observers. Observers will become an important and integral part of the system.

A fully functional online voting system on the blockchain will contain mathematical algorithms in the smart contract environment, allowing to achieve the anonymity of each voter, hide intermediate results, calculate encrypted voting data, analyze voting results in any aspect and to any depth up to a single vote.

This technology, along with legislative changes in the electoral system, information support, and education, will provide an opportunity to move from the current state of skepticism and mistrust to safe, transparent, and permanent election results. will restore voters' confidence in the electoral system of the Republic of Guatemala.